

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

CONTRIBUIÇÕES TÉCNICAS

Aperfeiçoamento do Edital nº 001/2026

Sandbox Regulatório SESP/PR – Segurança Pública na Faixa de Fronteira

Documento de contribuição institucional

Propostas técnicas voltadas à interoperabilidade, governança de inteligência artificial, proteção de dados, cadeia de custódia digital, integração operacional e avaliação objetiva das soluções participantes.

M.I. Montreal Informática S.A.

Responsável técnico: Adriano Messias Carpinetti de Oliveira
Head de Inovação – DSTEC

Julho de 2026

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

Carta de Apresentação

Prezados membros da Comissão do Sandbox Regulatório da Secretaria de Estado da Segurança Pública do Paraná,

A M.I. Montreal Informática S.A. apresenta, por meio deste documento, contribuições técnicas para o aperfeiçoamento da minuta do Edital nº 001/2026 e de seus anexos, relativos ao ambiente regulatório experimental de tecnologias aplicadas à segurança pública, com ênfase na faixa de fronteira do Estado do Paraná.

As sugestões foram elaboradas a partir da experiência da empresa em projetos de missão crítica, transformação digital, biometria, visão computacional, inteligência artificial, integração de sensores, aplicações móveis, comando e controle e gestão de evidências digitais.

O objetivo é colaborar para que o Sandbox estabeleça um ambiente seguro, auditável e operacionalmente útil para testar soluções inovadoras, preservando a autonomia tecnológica, a proteção dos direitos fundamentais e a capacidade de integração com a infraestrutura existente.

As propostas não buscam direcionar o chamamento a fornecedores ou tecnologias específicas. Ao contrário, priorizam requisitos funcionais, padrões abertos, métricas verificáveis, governança e resultados operacionais mensuráveis.

Atenciosamente,

Adriano Messias Carpinetti de Oliveira

Head de Inovação – DSTEC

M.I. Montreal Informática S.A.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

Sumário

1. Resumo Executivo
2. Princípios Orientadores
3. Sugestões Gerais ao Edital
4. Interoperabilidade e Arquitetura Aberta
5. Governança de Inteligência Artificial
6. Proteção de Dados e Segurança da Informação
7. Cadeia de Custódia Digital
8. Integração Operacional de Dispositivos e Sensores
9. Plano de Testes e Indicadores
10. Capacitação, Supervisão Humana e Gestão da Mudança
11. Soberania Tecnológica, Licenciamento e Código Aberto
12. Plano de Descontinuidade e Portabilidade
13. Matriz de Indicadores Recomendados
14. Conclusão

Tecnologia para um mundo mais seguro, eficiente e conectado.

1. Resumo Executivo

A minuta do Edital nº 001/2026 apresenta uma estrutura consistente para selecionar e acompanhar soluções de tecnologia aplicadas à segurança pública na faixa de fronteira. O texto contempla requisitos de inovação, maturidade tecnológica, capacidade operacional, gestão de riscos, proteção de dados, supervisão humana, interoperabilidade e descontinuidade.

As contribuições deste documento concentram-se em transformar esses requisitos em critérios ainda mais objetivos, verificáveis e comparáveis durante a seleção e a experimentação. A principal recomendação é que cada proposta seja avaliada não apenas por suas funcionalidades declaradas, mas por evidências técnicas, indicadores, protocolos de teste e mecanismos de auditoria.

Síntese das recomendações

Adotar requisitos mínimos de integração; exigir documentação de APIs; estabelecer métricas para modelos de IA; prever trilhas de auditoria e cadeia de custódia; diferenciar dados operacionais de evidências; padronizar testes em ambiente controlado e real; e garantir portabilidade, reversibilidade e exclusão segura ao término do piloto.

- Interoperabilidade por APIs documentadas, mensageria e padrões de dados.
- Governança de IA com supervisão humana, registro de decisões e monitoramento de vieses.
- Proteção de dados desde a concepção, com minimização, segregação e retenção definida.
- Cadeia de custódia digital para imagens, vídeos, áudios, documentos e resultados analíticos.
- Indicadores técnicos e operacionais previamente definidos e validados pela Comissão.
- Capacitação dos operadores e procedimentos claros para falhas, contestação e descontinuidade.

Tecnologia para um mundo mais seguro, eficiente e conectado.

2. Princípios Orientadores

Recomenda-se que a versão final do edital consolide um conjunto de princípios técnicos aplicáveis a todas as soluções, independentemente do fornecedor, modelo de licenciamento ou tecnologia utilizada.

Princípio	Aplicação recomendada
Interoperabilidade	Capacidade de integração com sistemas estaduais e federais, por meio de interfaces documentadas e padrões reconhecidos.
Segurança por padrão	Controles de acesso, criptografia, registro de eventos, segregação de ambientes e gestão de vulnerabilidades desde a concepção.
Privacidade por padrão	Tratamento mínimo e proporcional de dados pessoais, com finalidade definida, retenção limitada e descarte comprovável.
Supervisão humana	Decisões automatizadas devem apoiar, e não substituir, a análise do agente público quando houver impacto sobre direitos.
Auditabilidade	Resultados, parâmetros, versões, usuários, entradas e saídas devem ser rastreáveis.
Portabilidade	Dados e registros produzidos durante o piloto devem ser exportáveis em formato documentado.
Neutralidade tecnológica	Requisitos devem descrever capacidades e resultados, evitando dependência desnecessária de marcas específicas.
Evidência mensurável	Alegações de desempenho devem ser demonstradas por testes, relatórios e métricas reproduzíveis.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

3. Sugestões Gerais ao Edital

3.1. Glossário técnico comum

Sugestão	Glossário técnico comum
Redação/medida proposta	Incluir no edital ou em guia complementar um glossário mínimo com termos como evento, alerta, evidência, dado bruto, dado derivado, modelo, inferência, biometria, falsa correspondência, falso alerta, cadeia de custódia, trilha de auditoria, sensor, dispositivo de borda e ambiente controlado.
Justificativa	A padronização reduz interpretações divergentes entre proponentes, avaliadores e unidades operacionais.
Impacto esperado	Maior comparabilidade entre propostas e redução de ambiguidades contratuais.

3.2. Classificação de risco das soluções

Sugestão	Classificação de risco das soluções
Redação/medida proposta	Adotar classificação de risco técnico e de impacto sobre direitos, considerando finalidade, tipo de dado, autonomia da decisão, abrangência operacional, possibilidade de erro e reversibilidade.
Justificativa	Nem todas as soluções apresentam o mesmo nível de risco. A classificação permite definir controles proporcionais.
Impacto esperado	Aplicação objetiva de supervisão, auditoria, testes e requisitos de proteção de dados.

3.3. Evidências de maturidade tecnológica

Sugestão	Evidências de maturidade tecnológica
Redação/medida proposta	Solicitar demonstrações, relatórios de testes, referências de implantação, protótipos funcionais ou evidências equivalentes para comprovação do TRL declarado.
Justificativa	Evita que a avaliação se baseie apenas em material comercial ou declaração unilateral.
Impacto esperado	Seleção de soluções efetivamente aptas ao piloto.

3.4. Plano de integração obrigatório

Sugestão	Plano de integração obrigatório
Redação/medida proposta	Incluir no Plano de Trabalho uma matriz contendo sistemas envolvidos, finalidade da integração, dados trocados, protocolo, autenticação, frequência, responsável e estratégia de contingência.
Justificativa	Integrações são determinantes para o sucesso operacional e para o custo de implantação.
Impacto esperado	Redução de atrasos e riscos durante a experimentação.

4. Interoperabilidade e Arquitetura Aberta

A interoperabilidade deve ser tratada como requisito técnico mensurável. Recomenda-se que a Comissão solicite uma arquitetura lógica, uma matriz de integrações e a documentação mínima das interfaces necessárias ao piloto.

4.1. Documentação mínima de APIs

Sugestão	Documentação mínima de APIs
Redação/medida proposta	Exigir especificação de autenticação, endpoints, parâmetros, exemplos de requisição e resposta, códigos de erro, limites de uso, versionamento, política de depreciação e requisitos de segurança. Recomenda-se OpenAPI ou padrão equivalente.
Justificativa	A simples afirmação de que a solução possui API não garante integração viável.
Impacto esperado	Integrações mais rápidas, auditáveis e reutilizáveis.

4.2. Padrões de dados

Sugestão	Padrões de dados
Redação/medida proposta	Recomendar JSON, XML ou formatos abertos equivalentes; data e hora em ISO 8601; coordenadas geográficas em padrão documentado; identificadores únicos; codificação UTF-8; e metadados mínimos para mídia digital.
Justificativa	Padronização melhora portabilidade, correlação e uso por diferentes órgãos.
Impacto esperado	Menor dependência de fornecedor e melhor qualidade dos dados.

4.3. Integração assíncrona e eventos

Sugestão	Integração assíncrona e eventos
Redação/medida proposta	Prever, quando aplicável, suporte a webhooks, filas ou barramentos de eventos, com confirmação de entrega, retentativa e idempotência.
Justificativa	Soluções de segurança pública operam em tempo real e não devem depender apenas de consultas manuais.
Impacto esperado	Redução de perda de eventos e melhoria da resiliência.

4.4. Ambiente de homologação

Sugestão	Ambiente de homologação
Redação/medida proposta	Solicitar ambiente de testes separado do ambiente operacional, com dados sintéticos, anonimizados ou controlados e credenciais próprias.
Justificativa	Permite validar integrações e atualizações sem afetar a operação real.
Impacto esperado	Maior segurança e previsibilidade durante o piloto.

Tecnologia para um mundo mais seguro, eficiente e conectado.

5. Governança de Inteligência Artificial

A governança de inteligência artificial deve abranger o ciclo completo do modelo: finalidade, dados de entrada, treinamento, validação, implantação, monitoramento, atualização, contestação e desativação.

5.1. Ficha técnica do modelo

Sugestão	Ficha técnica do modelo
Redação/medida proposta	Exigir documento com finalidade, versão, responsável, dados de validação, limitações conhecidas, métricas, condições inadequadas de uso, dependências e data da última avaliação.
Justificativa	Facilita a análise técnica, o monitoramento e a responsabilização.
Impacto esperado	Transparência e rastreabilidade do componente algorítmico.

5.2. Supervisão humana por nível de risco

Sugestão	Supervisão humana por nível de risco
Redação/medida proposta	Determinar que alertas ou correspondências que possam provocar abordagem, restrição ou investigação sejam validados por operador autorizado, com registro da decisão e da justificativa.
Justificativa	Reduz o risco de decisões exclusivamente automatizadas com impacto sobre direitos.
Impacto esperado	Maior segurança jurídica e operacional.

5.3. Métricas por caso de uso

Sugestão	Métricas por caso de uso
Redação/medida proposta	Definir métricas adequadas a cada tecnologia: precisão, revocação, F1, taxa de falso positivo, taxa de falso negativo, tempo de resposta, disponibilidade e desempenho em condições adversas.
Justificativa	Uma única métrica pode ocultar limitações relevantes.
Impacto esperado	Avaliação objetiva e compatível com a finalidade operacional.

5.4. Monitoramento de deriva e atualização

Sugestão	Monitoramento de deriva e atualização
Redação/medida proposta	Exigir procedimento para identificar queda de desempenho, mudança de distribuição dos dados, atualização do modelo e eventual reversão de versão.
Justificativa	Modelos podem degradar em ambientes diferentes daqueles utilizados na validação.
Impacto esperado	Continuidade do desempenho durante o experimento.

5.5. Mitigação de vieses

Sugestão	Mitigação de vieses
Redação/medida proposta	Solicitar avaliação segmentada, quando tecnicamente aplicável e juridicamente autorizada, considerando condições de iluminação, ângulo, resolução, distância, idade aparente, uso de acessórios e outros fatores relevantes ao caso de uso.
Justificativa	Vieses podem decorrer tanto de atributos pessoais quanto das condições de captura.
Impacto esperado	Identificação mais precisa de limitações e definição de controles compensatórios.

6. Proteção de Dados e Segurança da Informação

O RIPD preliminar deve ser conectado ao Plano de Trabalho, à arquitetura e aos fluxos de dados. Recomenda-se evitar documentos genéricos que não identifiquem claramente finalidades, bases legais, categorias de titulares e medidas de proteção.

6.1. Mapa de dados

Sugestão	Mapa de dados
Redação/medida proposta	Exigir inventário dos dados tratados, origem, finalidade, base legal, compartilhamentos, local de armazenamento, prazo de retenção, responsável e procedimento de descarte.
Justificativa	Permite avaliar a proporcionalidade e reduzir tratamentos desnecessários.
Impacto esperado	Melhor governança e conformidade com a LGPD.

6.2. Segregação de dados e ambientes

Sugestão	Segregação de dados e ambientes
Redação/medida proposta	Determinar separação entre desenvolvimento, homologação e produção; entre dados operacionais e dados de demonstração; e entre bases de diferentes finalidades.
Justificativa	Reduz risco de acesso indevido, uso incompatível ou mistura de bases.
Impacto esperado	Maior controle e redução da superfície de exposição.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

6.3. Controles mínimos de segurança

Sugestão	Controles mínimos de segurança
Redação/medida proposta	Prever autenticação multifator para perfis sensíveis, princípio do menor privilégio, criptografia em trânsito e repouso, gestão de chaves, logs protegidos, backup testado e plano de resposta a incidentes.
Justificativa	Transforma requisitos genéricos de segurança em controles verificáveis.
Impacto esperado	Maior resiliência e proteção das informações.

6.4. Notificação de incidentes

Sugestão	Notificação de incidentes
Redação/medida proposta	Definir canal, responsáveis, conteúdo mínimo e prazos escalonados para comunicação de incidentes à SESP/PR, preservadas as obrigações legais aplicáveis.
Justificativa	A comunicação rápida é essencial para conter danos e preservar evidências.
Impacto esperado	Resposta coordenada e melhor gestão de riscos.

6.5. Residência e acesso a dados

Sugestão	Residência e acesso a dados
Redação/medida proposta	Exigir declaração sobre os locais de armazenamento, processamento, backup e suporte técnico, inclusive acessos remotos realizados por terceiros.
Justificativa	A residência física dos dados não é suficiente sem governança sobre quem pode acessá-los.
Impacto esperado	Maior aderência ao critério de soberania tecnológica.

Tecnologia para um mundo mais seguro, eficiente e conectado.

7. Cadeia de Custódia Digital

Recomenda-se diferenciar claramente conteúdo operacional, dado analítico e evidência digital. Uma imagem usada para alerta em tempo real pode exigir tratamento distinto daquela formalmente incorporada a uma ocorrência ou investigação.

7.1. Identificador único e hash

Sugestão	Identificador único e hash
Redação/medida proposta	Cada item incorporado como evidência deve receber identificador único, hash criptográfico, data e hora confiáveis, origem, dispositivo, operador e referência ao caso ou ocorrência.
Justificativa	Assegura integridade e vinculação do item ao contexto correto.
Impacto esperado	Preservação da autenticidade e capacidade de verificação posterior.

7.2. Original imutável e cópias de trabalho

Sugestão	Original imutável e cópias de trabalho
Redação/medida proposta	Preservar o arquivo original e registrar toda cópia, transcodificação, extração de quadro, melhoria de imagem ou análise realizada.
Justificativa	Evita confusão entre conteúdo original e material derivado.
Impacto esperado	Melhor admissibilidade e transparência pericial.

7.3. Trilha de custódia

Sugestão	Trilha de custódia
Redação/medida proposta	Registrar recebimento, transferência, acesso, exportação, compartilhamento, alteração de metadados, análise e descarte, com identidade do usuário e horário.
Justificativa	A cadeia de custódia depende do histórico completo de manipulação.
Impacto esperado	Rastreabilidade operacional e jurídica.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

7.4. Sincronização temporal

Sugestão	Sincronização temporal
Redação/medida proposta	Prever sincronização dos equipamentos e sistemas com fonte de tempo confiável, documentando fuso horário e eventuais desvios.
Justificativa	Eventos de câmeras, drones, aplicativos e sensores precisam ser correlacionados temporalmente.
Impacto esperado	Reconstrução precisa da linha do tempo.

7.5. Exportação verificável

Sugestão	Exportação verificável
Redação/medida proposta	Permitir exportação da evidência acompanhada de manifesto, hash, metadados essenciais, histórico de custódia e ferramenta ou procedimento de verificação.
Justificativa	A evidência deve permanecer verificável fora da plataforma original.
Impacto esperado	Portabilidade e redução de dependência tecnológica.

8. Integração Operacional de Dispositivos e Sensores

Para dispositivos de captura, recomenda-se avaliar não apenas a conectividade, mas o ciclo completo de ativação, captura, transmissão, armazenamento, associação à ocorrência, contingência e auditoria.

8.1. Câmeras corporais

Sugestão	Câmeras corporais
Redação/medida proposta	Solicitar descrição de ativação manual e automática, armazenamento local, transmissão ao vivo, buffer pré-evento, geolocalização, sincronização, indicadores de gravação, política de retenção e vínculo com ocorrência.
Justificativa	A utilidade operacional depende do conjunto de controles, e não apenas da gravação.
Impacto esperado	Maior confiabilidade e melhor integração com a gestão de evidências.

8.2. Drones e sensores aéreos

Sugestão	Drones e sensores aéreos
Redação/medida proposta	Exigir telemetria, identificação da aeronave e operador, plano de missão, registros de voo, vídeo, georreferenciamento, contingência de comunicação e integração com a central.
Justificativa	Permite reconstruir e auditar a missão.
Impacto esperado	Uso mais seguro e probatório do conteúdo aéreo.

Tecnologia para um mundo mais seguro, eficiente e conectado.

8.3. Veículos e leitura de placas

Sugestão	Veículos e leitura de placas
Redação/medida proposta	Registrar placa lida, imagem de contexto, câmera, faixa, sentido, localização, data/hora, confiança e resultado da consulta, mantendo regras para descarte de leituras sem interesse.
Justificativa	Reduz falsos alertas e evita retenção indiscriminada.
Impacto esperado	Melhor qualidade investigativa e proteção de dados.

8.4. Operação desconectada

Sugestão	Operação desconectada
Redação/medida proposta	Para aplicativos móveis e dispositivos de campo, solicitar modo offline controlado, criptografia local, sincronização posterior, prevenção de duplicidade e tratamento de conflitos.
Justificativa	A conectividade na faixa de fronteira pode ser intermitente.
Impacto esperado	Continuidade operacional e integridade dos registros.

8.5. Alertas multicanal

Sugestão	Alertas multicanal
Redação/medida proposta	Permitir que alertas críticos sejam entregues por canais configuráveis, com confirmação de recebimento, escalonamento e registro de tratamento.
Justificativa	Evita que eventos relevantes permaneçam sem resposta.
Impacto esperado	Melhoria do tempo de reação.

9. Plano de Testes e Indicadores

Recomenda-se que cada piloto seja estruturado em quatro etapas: preparação, teste controlado, teste operacional e avaliação final. Cada etapa deve possuir critérios de entrada, critérios de saída, riscos, responsáveis e evidências.

9.1. Protocolo de teste antes da implantação

Sugestão	Protocolo de teste antes da implantação
Redação/medida proposta	Aprovar previamente casos de teste, dados, cenários, indicadores, critérios de sucesso, limites de segurança, responsáveis e procedimento de interrupção.
Justificativa	Evita mudança posterior dos critérios para favorecer resultados.
Impacto esperado	Avaliação reproduzível e transparente.

9.2. Linha de base

Sugestão	Linha de base
Redação/medida proposta	Medir o processo atual antes do piloto, incluindo tempo, custo, volume, taxa de retrabalho e limitações.
Justificativa	Sem linha de base, não é possível demonstrar ganho real.
Impacto esperado	Mensuração objetiva do benefício operacional.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

9.3. Amostragem representativa

Sugestão	Amostragem representativa
Redação/medida proposta	Definir amostras e cenários que reflitam iluminação, clima, distância, conectividade, movimento, ruído, diversidade de dispositivos e condições adversas.
Justificativa	Testes excessivamente controlados podem superestimar o desempenho.
Impacto esperado	Maior validade externa dos resultados.

9.4. Registro de incidentes e quase incidentes

Sugestão	Registro de incidentes e quase incidentes
Redação/medida proposta	Manter catálogo de falhas, indisponibilidades, falsos alertas, ações corretivas e situações em que controles impediram um dano.
Justificativa	Quase incidentes são fonte relevante de aprendizado regulatório.
Impacto esperado	Melhoria contínua e prevenção.

10. Capacitação, Supervisão Humana e Gestão da Mudança

10.1. Matriz de perfis e competências

Sugestão	Matriz de perfis e competências
Redação/medida proposta	O Plano de Treinamento deve identificar perfis, responsabilidades, competências mínimas, carga horária, avaliação e reciclagem.
Justificativa	O mesmo sistema pode exigir formação distinta para operador, supervisor, investigador, administrador e auditor.
Impacto esperado	Uso mais seguro e consistente.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

10.2. Procedimentos operacionais padronizados

Sugestão	Procedimentos operacionais padronizados
Redação/medida proposta	Exigir POPs para tratamento de alertas, validação humana, registro de decisão, contestação, escalonamento, falha do sistema e operação manual.
Justificativa	Transforma funcionalidades em práticas operacionais confiáveis.
Impacto esperado	Redução de variação e erros humanos.

10.3. Avaliação de usabilidade

Sugestão	Avaliação de usabilidade
Redação/medida proposta	Medir tempo de execução, taxa de erro, facilidade de aprendizado, clareza dos alertas e percepção dos usuários.
Justificativa	Uma solução tecnicamente robusta pode falhar por baixa usabilidade.
Impacto esperado	Maior adoção pelas forças de segurança.

10.4. Mecanismo de contestação

Sugestão	Mecanismo de contestação
Redação/medida proposta	Definir procedimento para revisão de resultado automatizado, correção de cadastro e registro de divergência.
Justificativa	A contestação é componente essencial da supervisão e da governança.
Impacto esperado	Maior confiabilidade e proteção de direitos.

11. Soberania Tecnológica, Licenciamento e Código Aberto

A exigência de padrões abertos pode ser fortalecida por uma distinção entre componentes desenvolvidos especificamente com recursos ou dados do piloto, componentes preexistentes e serviços de terceiros. Essa separação reduz incertezas e permite avaliar corretamente portabilidade e dependência.

11.1. Matriz de componentes e licenças

Sugestão	Matriz de componentes e licenças
Redação/medida proposta	Solicitar relação de módulos, titularidade, licença, dependências, restrições, custos, local de hospedagem e plano de substituição.
Justificativa	Permite avaliar a autonomia real e os riscos de descontinuidade.
Impacto esperado	Maior transparência sobre dependências tecnológicas.

11.2. Código desenvolvido no piloto

Sugestão	Código desenvolvido no piloto
Redação/medida proposta	Definir previamente quais artefatos específicos do piloto serão entregues, incluindo código de integração, documentação, esquemas de dados, scripts de implantação e testes.
Justificativa	Evita divergências sobre o alcance da abertura do código.
Impacto esperado	Reutilização e continuidade pela Administração.

Tecnologia para um mundo mais seguro, eficiente e conectado.

11.3. Interfaces abertas para componentes proprietários

Sugestão	Interfaces abertas para componentes proprietários
Redação/medida proposta	Quando houver componentes proprietários preexistentes, exigir APIs documentadas, exportação de dados, trilhas de auditoria e ausência de bloqueio à integração com alternativas.
Justificativa	A soberania pode ser preservada mesmo em arquiteturas híbridas, desde que haja controle e portabilidade.
Impacto esperado	Equilíbrio entre inovação, propriedade intelectual e autonomia estatal.

11.4. Plano de independência de fornecedor

Sugestão	Plano de independência de fornecedor
Redação/medida proposta	Solicitar procedimentos para exportação, migração, substituição de componentes e continuidade dos dados em caso de encerramento.
Justificativa	Reduz risco de aprisionamento tecnológico.
Impacto esperado	Sustentabilidade de longo prazo.

Tecnologia para um mundo mais seguro, eficiente e conectado.

12. Plano de Descontinuidade e Portabilidade

12.1. Inventário de encerramento

Sugestão	Inventário de encerramento
Redação/medida proposta	O plano deve listar sistemas, dispositivos, integrações, credenciais, dados, cópias, backups, logs e responsáveis afetados pelo encerramento.
Justificativa	Assegura que nenhum componente seja esquecido.
Impacto esperado	Desativação completa e auditável.

12.2. Revogação de acessos e segredos

Sugestão	Revogação de acessos e segredos
Redação/medida proposta	Prever revogação de contas, tokens, certificados, chaves, túneis, acessos remotos e credenciais de serviço.
Justificativa	A exclusão de dados não elimina riscos de acessos residuais.
Impacto esperado	Redução de risco após o piloto.

12.3. Comprovação de eliminação

Sugestão	Comprovação de eliminação
Redação/medida proposta	Estabelecer relatório de descarte com escopo, método, data, responsável, exceções legais e evidências de execução.
Justificativa	Transforma a eliminação em procedimento verificável.
Impacto esperado	Maior confiança e conformidade.

12.4. Transferência de conhecimento

Sugestão	Transferência de conhecimento
Redação/medida proposta	Incluir entrega de documentação final, inventário de configuração, lições aprendidas e sessão de transferência para as equipes designadas.
Justificativa	Preserva o aprendizado regulatório e técnico.
Impacto esperado	Aproveitamento institucional do piloto.

13. Matriz de Indicadores Recomendados

Indicador	Definição	Referência recomendada
Disponibilidade	Percentual de tempo em que a solução permanece operacional.	≥ 90% durante janelas planejadas, salvo justificativa do piloto.
Latência de alerta	Tempo entre captura do evento e disponibilidade do alerta ao operador.	Definido por caso de uso e ambiente.
Precisão operacional	Proporção de resultados corretos entre resultados emitidos.	Segmentada por cenário.
Taxa de falso alerta	Percentual de alertas descartados após validação humana.	Monitoramento contínuo.
Tempo de atendimento	Tempo entre alerta, ciência, despacho e tratamento.	Comparado à linha de base.
Integridade de evidências	Percentual de itens com hash, metadados e custódia completos.	Meta de 100% para evidências formalizadas.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

Indicador	Definição	Referência recomendada
Rastreabilidade	Percentual de ações críticas registradas com usuário, data e contexto.	Meta de 100%.
Continuidade offline	Percentual de operações sincronizadas sem perda ou duplicidade.	Meta definida no protocolo.
Usabilidade	Taxa de conclusão de tarefas e erros por perfil de usuário.	Comparação antes/depois do treinamento.
Incidentes de segurança	Quantidade, severidade, tempo de detecção e resposta.	Tendência e conformidade com SLA.
Portabilidade	Percentual de dados exportáveis e validados fora da plataforma.	Meta definida no Plano de Descontinuidade.
Satisfação dos usuários	Avaliação estruturada dos operadores e gestores.	Escala e meta definidas antes do piloto.

14. Conclusão

O Sandbox Regulatório da SESP/PR possui potencial para se consolidar como referência nacional na avaliação responsável de tecnologias aplicadas à segurança pública. Para alcançar esse objetivo, é essencial combinar abertura à inovação com requisitos claros de segurança, governança, interoperabilidade, mensuração e proteção de direitos.

As contribuições apresentadas buscam apoiar a Comissão na transformação de princípios amplos em critérios técnicos verificáveis. A adoção dessas recomendações poderá facilitar a comparação entre propostas, reduzir riscos durante a experimentação, melhorar a qualidade das evidências produzidas e ampliar a possibilidade de reutilização dos resultados pela Administração Pública.

A M.I. Montreal Informática S.A. permanece à disposição para esclarecer os pontos apresentados e participar de discussões técnicas relacionadas ao aperfeiçoamento do edital e à estruturação dos protocolos de experimentação.

MONTREAL

Tecnologia para um mundo mais seguro, eficiente e conectado.

Referências documentais analisadas

- Minuta do Edital nº 001/2026 – Sandbox Regulatório SESP/PR – Fronteira.
- Minuta dos Anexos I a X do Edital.
- Decreto Estadual nº 13.728/2026.
- Lei Estadual nº 20.744/2021.
- Regulamento da Audiência Pública.
- Resolução de formação da Comissão do Sandbox Regulatório.

Contato institucional

Adriano Messias Carpinetti de Oliveira
Head de Inovação – DSTEC
M.I. Montreal Informática S.A.